

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information Associated with the Cellphones Assigned
Call Numbers (561) 657-1986 and (561) 657-1987 That
is Stored at Premises Controlled by AT&T Mobility

Case No. **1:20-MJ-00561**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A. This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41.

located in the Southern District of Florida, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| Code Section | Offense Description |
|--|--|
| 18 U.S.C. 1028(a)(7); 1028A; 1343; 1349 | Unlawful transfer, possession, or use of a means of ID; aggravated ID theft; wire fraud; conspiracy to commit wire fraud |

The application is based on these facts:

See attached affidavit.

☒ Continued on the attached sheet.

☒ Delayed notice of 30 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I, an attorney for the government, certify that the information likely to be obtained is relevant to an ongoing investigation being conducted by TIGTA. See 18 U.S.C. §§ 3122(b), 3123(b).



Applicant's signature

Sean Williams, Special Agent, TIGTA

Printed name and title

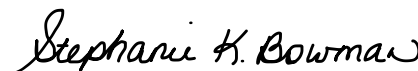


AUSA Julie D. Garcia

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

FaceTime Video (specify reliable electronic means).

Date: Jul 22, 2020



Judge's signature

City and state: Cincinnati, Ohio

Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title



ATTACHMENT A
Property to Be Searched

1. The following cellular telephones (collectively, the **TARGET CELL PHONES**):

TARGET CELL PHONE 1:

Call number: (561) 657-1986
Subscriber Name: P.J.²
IMSI: 310150925543986
ESN: 310150925543986

TARGET CELL PHONE 2:

Call number: (561) 657-1987
Subscriber Name: P.J.
IMSI: 310150925543987
ESN: 310150925543987

whose service provider is AT&T Mobility (AT&T), a wireless telephone service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, FL 33408.

2. All records and information associated with the **TARGET CELL PHONES** that are within the possession, custody, or control of the AT&T MOBILITY including information about the location of the cellular telephone if it is subsequently assigned a different call number.

² P.J.'s full name is redacted because he may be a victim of the fraud scheme under investigation.

ATTACHMENT B
Particular Things to be Seized

I. Information to be Disclosed by the Provider

1. All information about the location of the **TARGET CELL PHONES** described in Attachment A for a period of thirty days from the date of the warrant, during all times of day and night. “Information about the location of the **TARGET CELL PHONES**” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (*i.e.*, antenna towers covering specific geographic areas) and “sectors” (*i.e.*, faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

2. To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of AT&T MOBILITY, AT&T MOBILITY is required to disclose the Prospective Location Information to the government. In addition, AT&T MOBILITY must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Prospective Location Information unobtrusively and with a minimum of interference with AT&T MOBILITY’s services, including by initiating a signal to determine the location of the **TARGET CELL PHONES** on AT&T MOBILITY’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate AT&T MOBILITY for reasonable expenses incurred in furnishing such facilities or assistance.

3. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information.

See 18 U.S.C. § 3103a(b)(2).

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud) involving MICHAEL JOSEPH, VICTOR TORRES, ADESH BISSOON, and other unidentified coconspirators, including evidence of the identity of the user(s) associated with the device.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by AT&T MOBILITY in order to locate the things particularly described in this warrant.

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO**

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THE CELL PHONES ASSIGNED CALL
NUMBERS (561) 657-1986 AND (561)
657-1987 THAT IS STORED AT
PREMISES CONTROLLED BY AT&T
MOBILITY

Case No. 1:20-MJ-00561

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Sean Williams being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) for information about the location of the following cellular telephones (collectively, the “**TARGET CELL PHONES**”):

TARGET CELL PHONE 1:

Call number: (561) 657-1986
Subscriber Name: P.J.¹
IMSI: 310150925543986
ESN: 310150925543986

TARGET CELL PHONE 2:

Call number: (561) 657-1987
Subscriber Name: P.J.
IMSI: 310150925543987
ESN: 310150925543987

¹ As described below, I believe that P.J. is a victim of the identity-theft scheme described in this affidavit, so I have redacted P.J.’s full name for privacy reasons.

2. The service provider for the **TARGET CELL PHONES** is AT&T Mobility (“AT&T”), a wireless telephone service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, FL 33408. The **TARGET CELL PHONES** are further described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

3. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a “pen register” and/or “trap and trace device,” *see* 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. *See* 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. *See* 18 U.S.C. § 3123(b)(1).

4. I am a Special Agent with the United States Treasury Department, Treasury Inspector General for Tax Administration (“TIGTA”). TIGTA is tasked with ensuring the integrity of the Internal Revenue Service (“IRS”) and its infrastructure security and protecting the IRS against external attempts to corrupt tax administration. TIGTA special agents are certified criminal investigators with authority to carry firearms, make arrests, execute warrants, and administer oaths. I am assigned as a Criminal Investigator within the Cincinnati Field Office. I am also a member of TIGTA’s Cyber Investigative Cadre, whose mission is focused on communications- and computer network-related investigations. I have been employed by TIGTA since 2018. Prior to my employment with TIGTA, I was a special agent, investigator, and police officer with multiple U.S. federal government agencies. I have received training from the National Cyber-Forensics and Training Alliance and TIGTA’s Cybercrimes Investigative Division. Through my training and experience with

these types of investigations, I have encountered a number of situations where email, the Internet, and other technologies have been employed to conduct criminal activity. As a Special Agent, I continue to receive training and education related to the investigation and prosecution of computer and other high-tech related crimes.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028(a)(7) (Identity Theft), 1028A (Aggravated Identity Theft), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud), among others, have been, are being, and will be committed by the user of the **TARGET CELL PHONES** and other co-conspirators known and unknown. There is also probable cause to believe that the information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of individuals who are engaged in the commission of these offenses.

6. This Court has jurisdiction to issue the requested warrant because it is a “court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a “district court of the United States . . . that . . . has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

- A. The government is investigating a suspected identity-theft scheme in which multiple subjects have exchanged stolen PII and fraudulent documents by email.**

7. The U.S. Attorney's Office for the Southern District of Ohio and TIGTA are investigating a suspected identity-theft ring in which victims' stolen personally identifiable information (PII) is being shared between multiple subjects via email.

8. In 2019, search warrants were executed on email accounts used by suspect VICTOR TORRES. I reviewed the returns associated with these search warrants and found that TORRES's email accounts had exchanged emails containing lists of many individuals' PII and/or fraudulent identity documents (such as fraudulent Social Security cards) with various email addresses, including ZazaRoro24@gmail.com and KeystoneInc11@gmail.com. Some of the emails containing what appeared to be stolen PII dated back to 2011.

9. Based on my training and experience, the lists of PII and the fraudulent identity documents exchanged between these email accounts are consistent with a conspiracy to commit identity theft. Parallel investigations by TIGTA have shown that these types of materials have been used to open bank accounts and credit cards, and to apply for loans without authorization.

10. Based on the investigation to date, including the information described below, I believe that the identity-theft conspiracy described in this affidavit involves at least three co-conspirators: TORRES, MICHAEL JOSEPH—who I believe is the user of the **TARGET CELL PHONES**—and ADESH BISSOON.

B. In January 2020, agents executed a search warrant at TORRES's residence and found evidence that the user of the TARGET CELL PHONES is coconspirator MICHAEL JOSEPH.

11. In January 2020, a search warrant was executed at TORRES's residence in Apollo Beach, Florida. During the search, agents discovered fraudulent credit cards, checks, driver's licenses, and other fraudulent documentation. I believe based on this evidence that TORRES and his co-conspirators were still engaged in identity theft as of January 2020.

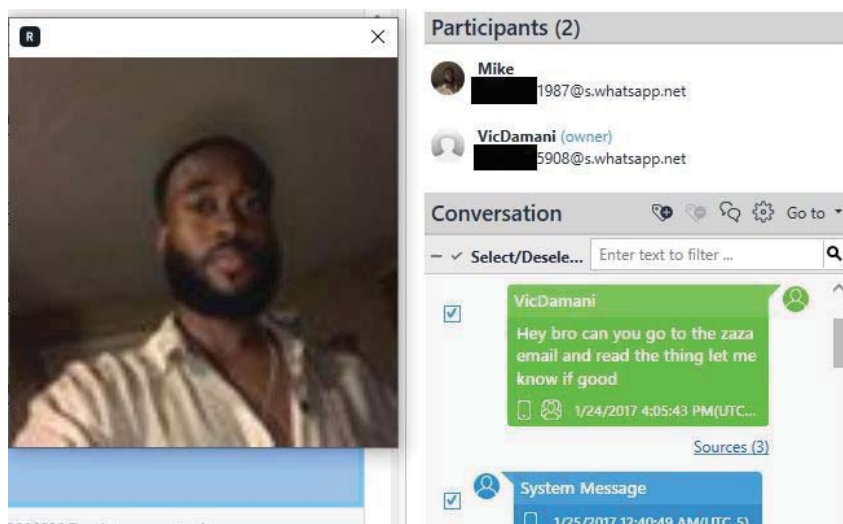
12. During the examination of VICTOR TORRES's telephone, agents found messages between TORRES and the **TARGET CELL PHONES**, sent using the messaging service WhatsApp. I believe that the same person uses both of the **TARGET CELL PHONES**, because the first six numbers of **TARGET CELL PHONE 1** and **TARGET CELL PHONE 2** are identical, and the last digits are sequential. Additionally, as noted above, both of the **TARGET CELL PHONES** are subscribed to P.J. (whose full name I have redacted for privacy).

13. The name associated with the contact in TORRES's phone for **TARGET CELL PHONE 2** was "MIKE." The messages exchanged between TORRES's phone and **TARGET CELL PHONE 2** included a reference to "the zaza email," which I believe was a reference to ZazaRoro24@gmail.com, one of the email accounts with which TORRES's accounts exchanged PII and fraudulent identity documents.

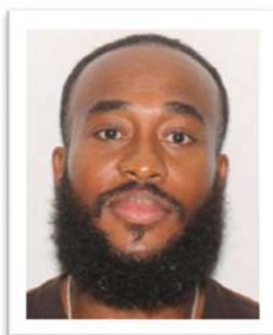
14. TORRES and the user of **TARGET CELL PHONE 2** also exchanged messages including requests to "Make a SSN" and "Do one DL & SS," as well as the PII of multiple individuals. I believe, based on my training and experience and knowledge of this investigation, including the information discussed below, that when TORRES and the user

of **TARGET CELL PHONE 2** referred to “do[ing]” or “mak[ing]” an “SSN” or “SS,” they meant creating a fraudulent Social Security Card.

15. The screenshot below shows the profile picture for “MIKE,” the user associated with **TARGET CELL PHONE 2**, as well as an example message from TORRES to “MIKE” mentioning “the zaza email”:

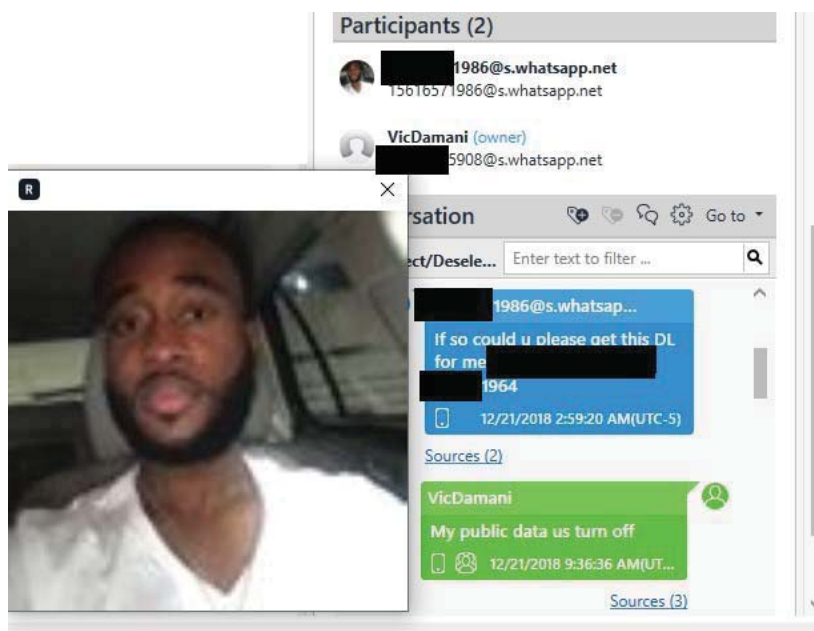


16. For reasons given in the following sections of this affidavit, and because the profile picture for “MIKE” appears to depict the same person, I believe that “MIKE” is MICHAEL JOSEPH, whose driver’s license photo is below:



17. As with **TARGET CELL PHONE 2**, the messages exchanged between TORRES’s phone and the **TARGET CELL PHONE 1** included messages that I believe

were about the creation of fraudulent identity documents. For example, I reviewed a message from **TARGET CELL PHONE 1** that read in part, “[C]ould u please get this DL for me: [Victim’s name redacted]; [month and day redacted]-1964.” A screenshot of this exchange is pictured below.



18. I believe based on my training and experience and knowledge of this investigation, including information described below, that when the user of **TARGET CELL PHONE 1** asked TORRES to “please get this DL for me” and then sent someone’s full name and date of birth, he was asking TORRES to create a fraudulent driver’s license using a victim’s PII.

19. The photograph on the left side of the screenshot above is the profile picture associated with **TARGET CELL PHONE 1**. Because this photograph appears to match that associated with **TARGET CELL PHONE 2**, which is under the name “MIKE”; because both of those photographs appear to match JOSEPH’s driver’s license photo; because the user of the **TARGET CELL PHONE 1**, like the user of **TARGET CELL**

PHONE 2, discussed with TORRES the creation of fraudulent identity documents; and because the phone numbers are identical except for the final digit (-1987 vs. -1986), I believe that the same person—JOSEPH—uses both numbers.

20. Additionally, both **TARGET CELL PHONE 1** and **TARGET CELL PHONE 2** are associated with Cricket Wireless billing account XXXXX1732. The name on this account is “P.J.” (whose full name I have redacted for privacy). I believe P.J. may be a victim of the identity-theft scheme, because in September 2016 his PII was emailed from JOSEPH to BISSOON). Payments to this account were made with credit cards in the names of P.J.; another person I believe to be a victim, whose initials are J.M.; and MICHAEL JOSEPH.

21. In addition to the foregoing evidence, I believe that JOSEPH is the user of ZazaRoro24@gmail.com because I obtained a search warrant for the account found that it contained multiple documents with JOSEPH’s personal information, including one email titled “My Info,” which listed JOSEPH’s name, Keystone Green Technology (a company registered to JOSEPH), JOSEPH’s known addresses, the last four digits of JOSEPH’s SSN, and a weekly and hourly pay rate. I believe this information was used to create fraudulent pay stubs for JOSEPH; I have found examples of such documents in other email accounts during this investigation.

22. Information from AT&T shows that the **TARGET CELL PHONES** were activated in 2017 under P.J.’s name. At least as of March 2020, the **TARGET CELL PHONES** were still subscribed in the name of P.J. For that reason, I believe there is probable cause that JOSEPH continues to use the **TARGET CELL PHONES**.

23. I am now seeking a search warrant for location information associated with the **TARGET CELL PHONES** to assist agents in surveilling the user of the **TARGET CELL PHONES** for the purpose of obtaining additional evidence of the scheme under investigation, including definitively identifying the user(s) of the **TARGET CELL PHONES**.

BACKGROUND ON AT&T AND LOCATION INFORMATION

24. In my training and experience, I have learned that AT&T is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including E-911 Phase II data, also known as GPS data or latitude-longitude data, and cell-site data, also known as “tower/face information” or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device’s signal using data from several of the provider’s cell towers. Cell-site data identifies the “cell towers” (*i.e.*, antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (*i.e.*, face of the tower) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or GPS data.

25. Based on my training and experience, I know that AT&T can collect E-911 Phase II data about the location of the **TARGET CELL PHONES**, including by initiating a signal to determine the location of the **TARGET CELL PHONES** on AT&T's network or with such other reference points as may be reasonably available.

26. Based on my training and experience, I know that AT&T can collect cell-site data about the **TARGET CELL PHONES**. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as AT&T typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

AUTHORIZATION REQUEST

27. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

28. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the **TARGET CELL PHONES** would seriously jeopardize the

ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

29. I further request that the Court direct AT&T to disclose to the government any information described in Attachment B that is within the possession, custody, or control of AT&T. I also request that the Court direct AT&T to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with AT&T's services, including by initiating a signal to determine the location of the **TARGET CELL PHONES** on AT&T's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate AT&T for reasonable expenses incurred in furnishing such facilities or assistance.

//

//

//

//

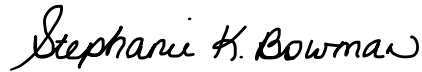
30. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the **TARGET CELL PHONES** outside of daytime hours.

Respectfully submitted,



Sean Williams
Special Agent
Treasury Inspector General for Tax
Administration (TIGTA)

Attested to by the Applicant in accordance with Fed. R. Crim. P. 4.1 this 22 day of July, 2020. **via Facetime Video.**



THE HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

1. The following cellular telephones (collectively, the **TARGET CELL PHONES**):

TARGET CELL PHONE 1:

Call number: (561) 657-1986
Subscriber Name: P.J.²
IMSI: 310150925543986
ESN: 310150925543986

TARGET CELL PHONE 2:

Call number: (561) 657-1987
Subscriber Name: P.J.
IMSI: 310150925543987
ESN: 310150925543987

whose service provider is AT&T Mobility (AT&T), a wireless telephone service provider headquartered at 11760 U.S. Highway 1, North Palm Beach, FL 33408.

2. All records and information associated with the **TARGET CELL PHONES** that are within the possession, custody, or control of the AT&T MOBILITY including information about the location of the cellular telephone if it is subsequently assigned a different call number.

² P.J.'s full name is redacted because he may be a victim of the fraud scheme under investigation.

ATTACHMENT B
Particular Things to be Seized

I. Information to be Disclosed by the Provider

1. All information about the location of the **TARGET CELL PHONES** described in Attachment A for a period of thirty days from the date of the warrant, during all times of day and night. “Information about the location of the **TARGET CELL PHONES**” includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information, as well as all data about which “cell towers” (*i.e.*, antenna towers covering specific geographic areas) and “sectors” (*i.e.*, faces of the towers) received a radio signal from the cellular telephone described in Attachment A.

2. To the extent that the information described in the previous paragraph (hereinafter, “Location Information”) is within the possession, custody, or control of AT&T MOBILITY, AT&T MOBILITY is required to disclose the Prospective Location Information to the government. In addition, AT&T MOBILITY must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Prospective Location Information unobtrusively and with a minimum of interference with AT&T MOBILITY’s services, including by initiating a signal to determine the location of the **TARGET CELL PHONES** on AT&T MOBILITY’s network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate AT&T MOBILITY for reasonable expenses incurred in furnishing such facilities or assistance.

3. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1028 (Identity Theft), 1028A (Aggravated Identity Theft), 1343 (Wire Fraud), and 1349 (Conspiracy to Commit Wire Fraud) involving MICHAEL JOSEPH, VICTOR TORRES, ADESH BISSOON, and other unidentified coconspirators, including evidence of the identity of the user(s) associated with the device.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by AT&T MOBILITY in order to locate the things particularly described in this warrant.